MAT 4930: Quantum Algorithms and Complexity **Spring 2021**

Lecture 11: Elementary Number Theory

Lecturer: Jean-François Biasse *TA: Robert Hart*

11.1 Modular arithmetic

When performing Shor's factoring algorithm, we need to compute arithmetic operations (multiplications and exponentiations) modulo the number N to be factored.

Definition 11.1 (Modular equivalence) *We say that $x, y \in \mathbb{Z}$ are equivalent modulo $N \in \mathbb{Z}_{>0}$ if*

$$N \mid (b-a).$$

We denote this by $a \equiv b \bmod N$.

Note that $a \equiv b \bmod N$ (which is an equivalence relation between a and b) should not be confused with the related notion of $a \bmod N$ which denotes the remainder of the integer division between a and N (which means that $a \bmod N$ is an integer in $\{0, \dots, N-1\}$. When we perform arithmetic operations modulo N, the elements we are dealing with are not technically speaking integers, but rather equivalence classes modulo N.

Definition 11.2 (Congruence class modulo N) *The congruence class of the integer a modulo N is*

$$\overline{a} := \{x \in \mathbb{Z} \ \text{ such that } \ x \equiv a \bmod N\}.$$

We also denote this $[a]$, or when there is a possibilty of confusion about the modulus, we can use $[a]_N$.

This means that our elements are in fact sets with an infinite number of elements. This might seem like extra complication at first, but for each integer $a \in \mathbb{Z}$ where is a distinguished element in $[a]$, namely $r = a \bmod N$, the remainder of the division of a by N.

Proposition 11.3 *Let $a \in \mathbb{Z}$ and $N \in \mathbb{Z}_{>0}$, there is one and only one element $x \in \{0, \dots, N-1\}$ such that*

$$x \equiv a \bmod N.$$

This element is necessarily $x = a \bmod N$.

The above means that the congruence classes modulo N are in one-to-one correspondance with integers in the set $\{0, \dots, N-1\}$. It is very frequent to identify $[a]$ by $a \bmod N$, but one needs to remember that $[a]$ is a set while $a \bmod N$ is an integer. Congruence classes modulo N form a ring that we denote by $\mathbb{Z}/N\mathbb{Z}$. This means that classes can be added and multiplied together by a straighforward procedure described in the following.

Definition 11.4 (Arithemtic in $\mathbb{Z}/N\mathbb{Z}$) *Let $[a]$ and $[b]$ be two congruence classes modulo N. Then we define their multiplication and additions by*

- $[a] + [b] := [a + b]$,
- $[a] \cdot [b] := [a \cdot b]$.

Example 1 *Let $N = 7$, and $a = 3$, $b = 4$. We have*

$$[a] + [b] = [3 + 4] = [7] = [0]$$
$$[a] \cdot [b] = [3\dot{4}] = [12] = [5]$$

For convenience and efficiency, we always strive to represent $[a]$ as $[r]$ (or simply r if there is no ambiguity) where $r = a \bmod N$. As congruence classes can be multiplied, they can also be exponentiated as well. Exponentiation will be a crucial part of Shor's factoring algorithm. In particular, we need to perform fast exponentiation. This means that given $x > 0$ and $[a]$, we want to find $a^x \bmod N$ in as few multiplications between elements of $\{0, \ldots, N-1\}$ as possible. The square-and-multiply strategy offers that possibilty. Assume that the binary decomposition of x is

$$x = x_0 + x_1 \cdot 2 + x_2 \cdot 2^2 + \ldots + x_k \cdot 2^k.$$

Then we perform the following operations

$$\begin{aligned}
[a]^2 &= [a] \cdot [a] \\
[a]^{2^2} &= [a]^2 \cdot [a]^2 \\
[a]^{2^3} &= [a]^{2^2} \cdot [a]^{2^2} \\
&\vdots \\
[a]^{2^k} &= [a]^{2^{k-1}} \cdot [a]^{2^{k-1}}
\end{aligned}$$

This provides $[a]^{2^i}$ for $i = 1, \ldots, k$ at the cost of k multiplications in $\mathbb{Z}/N\mathbb{Z}$. Then we use them to compute $[a]^x$ as follows

$$[a]^x = [a]^{x_0 + x_1 \cdot 2 + x_2 \cdot 2^2 + \ldots + x_k \cdot 2^k} = [a]^{x_0} \cdot \left([a]^2\right)^{x_1} \cdot \left([a]^{2^2}\right)^{x_2} \ldots \left([a]^{2^k}\right)^{x_k}.$$

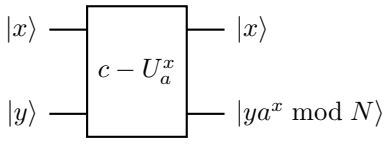
As the digits x_i are either 0 or 1, this means that the above product requires at most k multiplications in $\mathbb{Z}/N\mathbb{Z}$.

Example 2 *Suppose that $N = 23$, $a = 17$, and $x = 17$. Then first we notice that $x = 2^4 + 1$ (so that $k = 4$). Then we calculate*

$$\begin{aligned}
[a]^2 &= [17] \cdot [17] = [13] \\
[a]^{2^2} &= [13] \cdot [13] = [8] \\
[a]^{2^3} &= [8] \cdot [8] = [18] \\
[a]^{2^4} &= [18] \cdot [18] = [2]
\end{aligned}$$

Therefore, $[a]^x = [a]^{2^4} \cdot [a] = [17] \cdot [2] = [11]$.

Most importantly for Shor's algorithm, the above classical can be implemented by a quantum circuit following Bennett's result. This means that we can assume that we have the following building block that can be realized efficiently:



A last piece of theory that is important for what follows is the Chinese Remainder Theorem. This means that if $N = ab$ where a and b are coprimes, then congruence classes modulo N are in bijection with pairs of congruence classes modulo a and b.

Theorem 11.5 (Chinese Remainder Theorem (CRT)) *Let $N = ab$ where a and$b$ are coprime. Then we have the bijection*

$$\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}.$$

Example 3 *As an example, assume $a = 2$ and $b = 3$. Then the CRT tells us that $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. In particular, this means that the following system of simultaneous congruences*

$$x \equiv 1 \bmod 2$$
$$x \equiv 2 \bmod 3$$

has one and only one solution $x \in \{0, \ldots, 5\}$. There is an algorithm for properly computing it, but by direct analysis (the number involved are so small) we clearly see that $x = 5$ is our solution.

This can be immediately generalized by induction to the case of $N = a_1, \ldots, a_k$ where all a_i, a_j for $i \neq j$ are pairwise coprime. In this case, we have $\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_k\mathbb{Z}$.

11.2 Units modulo N

Shor's algorithm can be seen as a method for finding the order of an element in $(\mathbb{Z}/N)^*$, the group of units modulo N.

Definition 11.6 (Unit modulo N) *The congruence class $[a]$ (resp. the integer a) is said to be a unit modulo N if there exists an integer b such that*

$$[a] \cdot [b] = [1]$$

which is equivalent to $ab \equiv 1 \bmod N$.

Units modulo N form a multiplicative group. The elements of $(\mathbb{Z}/N)^*$ are in one-to-one correspondance with elements of $a \in \{0, \ldots, N-1\}$ that have an inverse modulo N. These are the elements coprime to N as we know by Bezout's lemma that if a is coprime with N, there are $u, v \in \mathbb{Z}$ such that $ua + vN = 1$, which shows that a is a unit (the converse is also true).

Proposition 11.7 *The elements of the group $(\mathbb{Z}/N)^*$ are in one-to-one correspondance with*

$$\{a \in \{0, \dots, N-1\} \quad \textit{such that} \quad \gcd(a, N) = 1\}$$

We denote by $\phi(N)$ the cardinality of the above set (and thus of $(\mathbb{Z}/N)^*$).

The order $\phi(N)$ of $(\mathbb{Z}/N)^*$ is called the Euler ϕ function. Its behavior is the topic of a lot of research in number theory. However, we know how to evaluate it at a given N very easily. Indeed, we take the following approach: first evaluate it at $N = p$ a prime. Then at numbers of the form $N = p^x$, and at arbitrary numbers. From Proposition 11.7, we clearly see that $\phi(p) = p - 1$ because aside from 0, all elements of $\{0, \dots, p-1\}$ are coprime with p (by definition of p being a prime). Then, the case of $N = p^x$ is barely more complicated. Indeed, by inspection, the only elements of $\{0, \dots, p^x\}$ that are not coprime with p^x are $0, p, 2p, 3, p, \dots, (p^{x-1} - 1)p$. That is p^{x-1} elements, and all the other $p^x - p^{x-1} = p^{x-1}(p-1) = \phi(p^x)$ elements are coprime to p^x.

Proposition 11.8 *Suppose $N = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}$ for distict primes p_i. The cardinality of $(\mathbb{Z}/N)^*$ satisfies*

$$\phi(N) = p_1^{x_1 - 1}(p_1 - 1) \cdot p_2^{x_2 - 1}(p_1 - 1) \dots p_k^{x_k - 1}(p_k - 1)$$

Proof: The formula clearly generalizes the case of $N = p$ and $N = p^x$. Assume now that N has an arbitrary prime decomposition. First, if $N = ab$ for a, b coprime, then by the CRT, $\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, and clearly, this bijection induces one on the corresponding unit groups:

$$(\mathbb{Z}/N\mathbb{Z})^* \simeq (\mathbb{Z}/b\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^* .$$

In particular, $\phi(N) = \phi(a)\phi(b)$. By induction, this implies that

$$\phi(N) = \phi\left(p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}\right) = \phi\left(p_1^{x_1}\right) \phi\left(p_2^{x_2}\right) \dots \phi\left(p_k^{x_k}\right) = p_1^{x_1 - 1}(p_1 - 1) \cdot p_2^{x_2 - 1}(p_1 - 1) \dots p_k^{x_k - 1}(p_k - 1).$$

■

Shor's algorithm, as we will see in the next lecture, aims to compute the order r of an element a modulo N, that is, to find the smallest positive integer r such that $[a]^r = [1]$ (or equivalently $a^r \equiv 1 \bmod N$. First of all, this task does not make sense if a is not coprime to N. The integer a is chosen uniformly at random in $\{0, \dots, N-1\}$. The GCD between N and a can be computed efficiently by the Euclidean algorithm, and if the result is not 1, then we found a non-trivial factor p of N and we can repeat the process with $N' = N/p$ (or stop there in the case where $N = pq$ is an RSA number). Once r is found, we have the following identity:

$$N \mid a^r - 1.$$

We hope that r is even (we'll calculate the odds of that happening below). If this is the case, then we have $(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \bmod N$, which means

$$N \mid (a^{r/2} - 1)(a^{r/2} + 1).$$

At this point, if we do not have $N \mid (a^{r/2} - 1)$, nor $N \mid (a^{r/2} - 1)$, then $\gcd(N, a^{r/2} - 1)$ must be a non trivial factor of N since it must be that $N = ab$ for $a, b \neq 1$ and $a \mid (a^{r/2} - 1)$ and $b \mid (a^{r/2} - 1)$.

Example 4 *Let $N = 15$. Then $4^2 \equiv 1 \bmod N$ and N does not divide $4-1$ nor $4+1$. Hence $\gcd(N, 4-1) = 3$ is a non-trivial factor of N.*

Proposition 11.9 *Let p be an odd prime and let a be drawn uniformly at random in $\{0, \dots, p-1\}$. Then the order r of a modulo N is even with probability at least $1/2$.*

Proof: It can be shown that for p a prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group. This means that there is $g \in \{0,\dots,p-1\}$ such that for all a in $\{0,\dots,p-1\}$ there is a unique $0 \leq k < p-1$ with $a \equiv g^k \bmod N$. When we draw a uniformly at random in $\{0,\dots,p-1\}$, k is odd with probability $1/2$. Then we have

$$a^r \equiv g^{rk} \equiv 1 \bmod N,$$

therefore $p-1 \mid rk$. Since $p-1$ is even, whenever k is odd, r has to be even as well. ■

Proposition 11.10 *Assume N is of the form $N = pq$ for p, q odd prime numbers (i.e. N is an RSA integer), and a in drawn uniformly at random in $\{0,\dots,p-1\}$. If $\gcd(a,N) = 1$, then with probability at least $3/8$, we have*

- *The order r of a modulo N is even,*
- *N does not divide $a^{r/2}-1$ nor $a^{r/2}+1$.*

Proof: By the CRT, choosing a at random is equivalent to choosing $a_1 \in \{0,\dots,p-1\}$ and $a_2 \in \{0,\dots,q-1\}$ uniformly at random. Clearly $a_1^r \equiv 1 \bmod p$ and $a_2^r \equiv 1 \bmod q$, therefore $r_1 \mid r$ and $r_2 \mid r$ where r_1 is the order of a_1 modulo p and r_2 is the order of a_2 modulo q. From Proposition 11.9, r_1 is even with probability $1/2$, and r_2 is even with probability $1/2$. Therefore, with probability $3/4$, one of r_1 or r_2 is even, which forces r to be even as well.

When we are in the case r even, we have $a^r = b^2$ for $b = a^{r/2}$. Additionally,

$$b^2 \equiv 1 \bmod p$$
$$b^2 \equiv 1 \bmod q.$$

There are only two square roots of 1 modulo a prime number: ± 1. By the CRT, this gives us 4 square roots of 1 modulo $N = pq$. So b is one of these 4 different square roots modulo N. Two of them are congruent to ± 1 modulo N, and since a is drawn uniformly at random, there is a probability $1/2$ that b is not congruent to ± 1 modulo N. In this case, N does not divide $a^{r/2}-1$ nor $a^{r/2}+1$. Overall, this happens with probabilty $\frac{3}{4} \times \frac{1}{2} = \frac{3}{8}$. ■

11.3 Continued fraction expansions

An important component of Shor's algorithm is the continued fraction expansion of a value measured at the end of the quantum circuit. We present here the essential facts regarding continued fractions to understand why this enables Shor's algorithm to perform its task. The continued fraction expansion of $x \in \mathbb{R}$ is sequence of rational numbers calculated from x. The elements of this sequence can be viewed as rational approximations of x. The process which goes like this:
1st step: $a_0 = \lfloor x \rfloor\,,\ n = a_0 + \epsilon_0,\ 0 \leq \epsilon_0 < 1$ So $x \sim a_0 \in \mathbb{Z},\ a_0 = p_0/q_0$

2nd step: $1/\epsilon_0 = a_1 + \epsilon_1$ where $a_1 = \lfloor 1/\epsilon_0 \rfloor\,,\ 0 \leq \epsilon_1 < 1$ so $x = a_0 + \frac{1}{a_1+\epsilon_1} \sim a_0 + 1/a_1 = p_1/q_1$.

3rd step: $1/\epsilon_1 = a_2 + \epsilon_2$ where $a_2 = \lfloor 1/\epsilon_1 \rfloor\,,\ 0 \leq \epsilon_1 < 1$ so

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2+\epsilon_2}} \sim a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{p_2}{q_2}$$

etc... The sequence $p_0/q_0,\ p_1/q_1,\ p_2/q_2, ...$ is the continued fraction expansion of x. It may be infinite (in fact, it has to be infinite if $x \notin \mathbb{Q}$). If $a_0, a_1, a_2, \ldots$ is the continued fraction expansion of x, we denote this by $x = [a_0, a_1, a_2, \ldots]$ or

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Definition 11.11 (Convergent) *If $\frac{p_i}{q_i}$ is of the form $[a_0, a_1, \ldots, a_i]$ where $[a_0, a_1, \ldots]$ is the continued fraction expansion of $x \in \mathbb{R}$, then we say that $\frac{p_i}{q_i}$ is the i-th convergent of the continued fraction expansion of x.*

A key ingredient in Shor's algorithm is the fact that if a rational number is close enough to x, then it must be a convergent of the continued fraction expansion of x.

Theorem 11.12 *Let x be a rational number, and suppose that p/q is a rational number such that*

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}.$$

Then p/q is a convergent of the continued fraction expansion of x.

Proof: Let $[a_0, \ldots, a_n]$ be the continued fraction expansion of p/q, and let p_i/q_i be its convergents for $i = 0, \ldots, n$ (in particular $p/q = p_n/q_n$). Let

$$\delta := 2q_n^2 (x - \frac{p_n}{q_n}).$$

We have $|\delta| < 1$ and $x = \frac{p_n}{q_n} + \frac{\delta}{2q_n^2}$. Now let

$$\lambda := 2 \left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n}.$$

We can show that

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}}$$

and therefore

$$x = [a_0, \ldots, a_n, \lambda] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\cdots}{\lambda}}}}$$

We can show by induction that

$$p_n = a_n p_{n-1} + p_{n-2}$$
$$q_n = a_n q_{n-1} + q_{n-2}.$$

In turn, this allows us to prove that $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ for $n \geq 1$. When n is even, $q_n p_{n-1} - p_n q_{n-1} = 1$ and thus

$$\lambda := 2 \left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n} = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 > 1.$$

Since λ is a rational number, we can write it as $\lambda = [b_0, \ldots, b_m]$ for positive integers $b_0, \ldots, b_m$. This means that $x = [a_0, \ldots, a_n, b_0, \ldots, b_m]$, and $\frac{p}{q} = [a_0, \ldots, a_n]$ is a convergent of x. ■